

# Máster en Programación avanzada en Python para Big Data, Hacking y Machine Learning

Hacking y Pentesting con Python

# MÓDULO 05

Librerías básicas para la automatización de procesos.

## Protocolos de acceso remoto.

Una de las labores básicas que debe realizar cualquier administrador de sistemas consiste precisamente en acceder a los servidores y ejecutar instrucciones que le permitan configurar software, instalar programas y gestionar los recursos del sistema.

Tradicionalmente el protocolo SSH ha sido utilizado precisamente para implementar dichas rutinas, sin embargo las medidas de seguridad ineficientes o directamente inexistentes sobre dichos servicios, les convierten en una herramienta perfecta para el acceso remoto de atacantes.

Aunque el protocolo como tal es seguro e implementaciones tan extendidas como OpenSSH han reportado pocas vulnerabilidades críticas, es posible que uno de estos servicios se encuentre mal configurado o sea útil para un atacante a la hora de realizar procesos de post-explotación.

## Acceso a servidores SSH con Paramiko.

Se trata de una librería que soporta el protocolo SSHv1 y SSHv2, permitiendo la creación de clientes y servidores SSH de forma fácil, rápida y segura.

Paramiko es una la librería de uso estándar en Python cuando se requiere utilizar protocolo SSH y depende de PyCrypto para todas las operaciones de cifrado.

Del mismo modo que las implementaciones OpenSSH o DropBear permiten la creación de túneles cifrados, Paramiko también soporta esta característica gracias a su potente API y un amplio conjunto de clases útiles para cumplir con dicho objetivo.

MUCHAS GRACIAS POR SU ATENCIÓN



decheverri@grupomainjobs.com



LINKEDIN

Daniel Echeverri

<https://www.linkedin.com/in/adastra1/>



twitter.com/eiposgrados



facebook.com/eiposgrados



instagram.com/eiposgrados